Hardware Evaluation of the AES Finalists

Tetsuya ICHIKAWA

Mitsubishi Electric Engineering Co.

Tomomi KASUYA, Mitsuru MATSUI

Mitsubishi Electric Corporation

Outline

1. **Overview**
2. **Design Policies**
3. **Hardware Evaluation Results**
4. **Discussions**
5. **Conclusions**

Overview(1)

We evaluated

the AES finalists, DES and Triple-DES

under the same hardware condition and environment using

our publicly available 0.35 micron CMOS ASIC design library

Overview(2)

Our evaluation results (encryption speed):

Rijndael > DES ≈ Serpent >

(≈ 2[Gbps]) (≈ 1[Gbps])

Triple-DES ≈ Twofish > Mars ≈ RC6

(≈ 400[Mbps]) (≈ 200[Mbps])

Design Policies
(our goal)

Our purpose is to evaluate the fastest possible encryption speed of the AES finalists (in feedback modes) using the existing hardware standard library under fair conditions.

Design Policies (Hardware architecture)

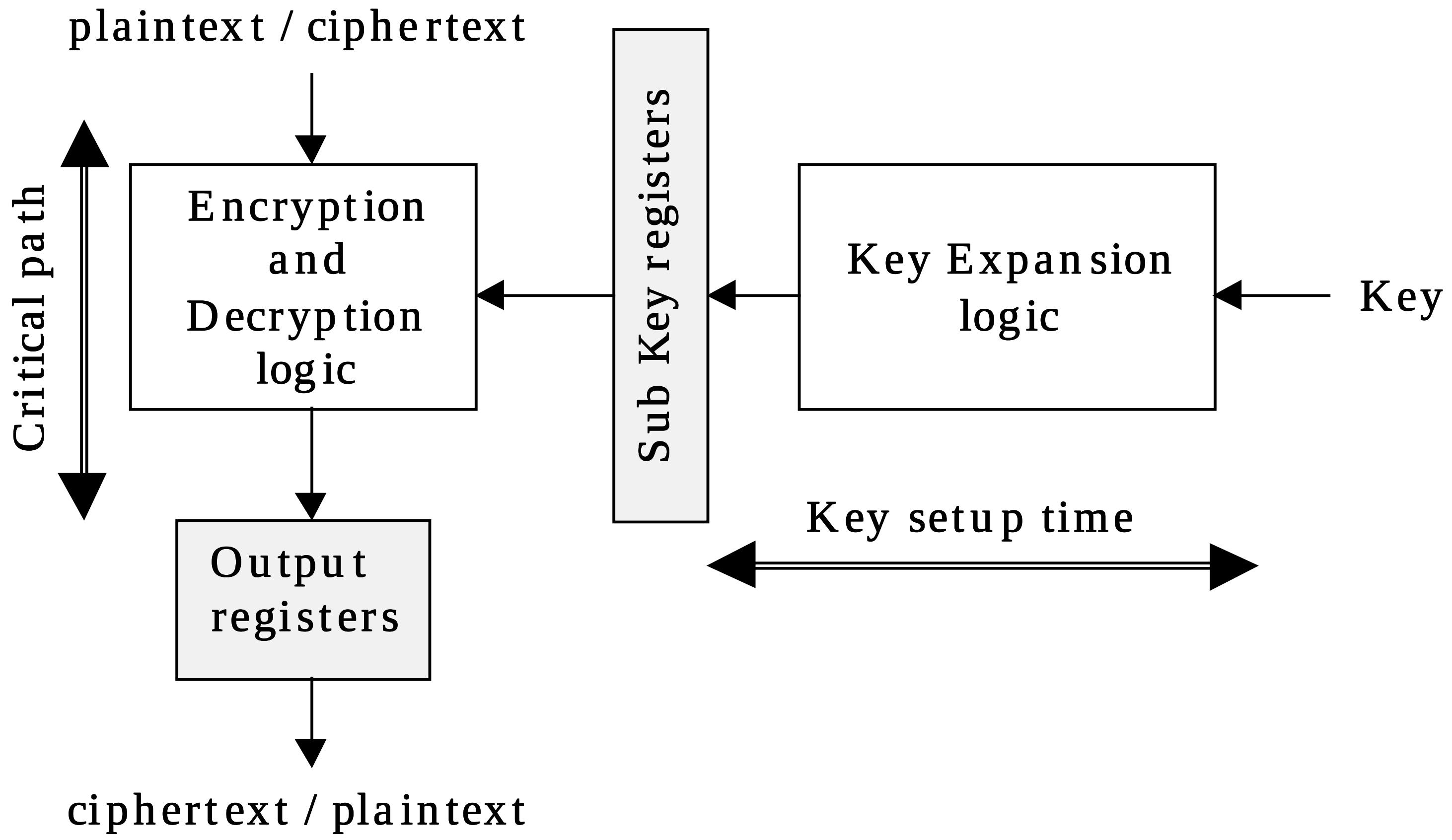
*We introduced the “subkey registers” for storing all subkey bits before an encryption operation.

*We did not adopt pipeline architecture.

*We introduced fully loop-unrolled architecture.

*We designed 128-bit key versions.

- *The Hardware Structure* -



- *Throughput (encryption speed)* -

Throughput[bps] =

128[bit] / critical path [sec]

- *Our design environment* -

*Language ... Verilog-HDL

*Simulator ... Verilog-XL

*Logic Synthesis ... Design Compiler
(version 1998-08)

*Design library ...
Mitsubishi 0.35 micron CMOS ASIC

Design Policies
(HDL description)

*We did not use a special optimization technique to design lookup tables in hardware.

*For arithmetic operations such as additions, subtractions and multiplications, we used the fastest ones in the library of Synopsys Design Ware Basic Library.

Design Policies
(hardware condition)

We adopted the

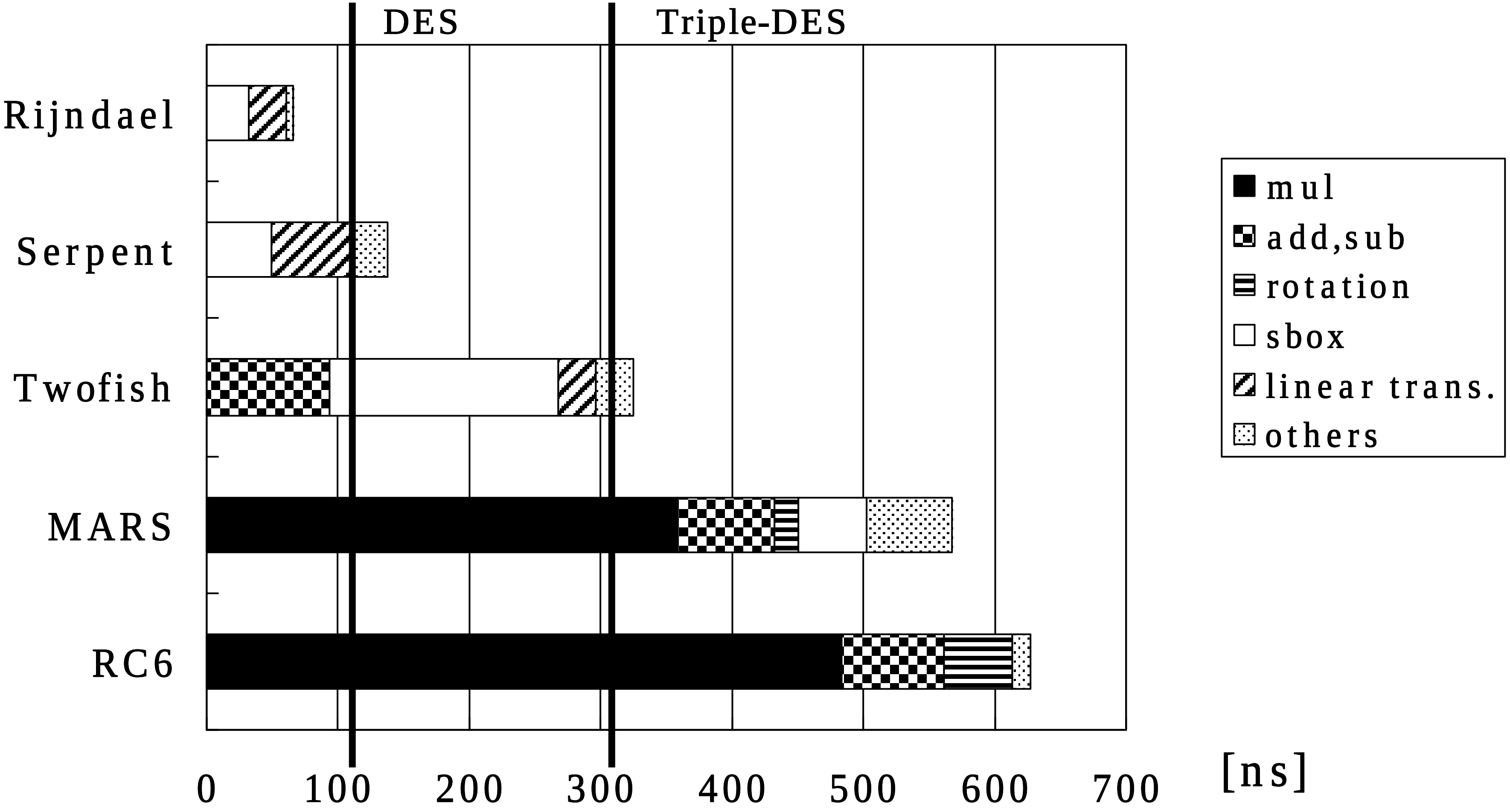
"*WORST (MAXIMUM) CASE"*

***hardware condition* for evaluation.**

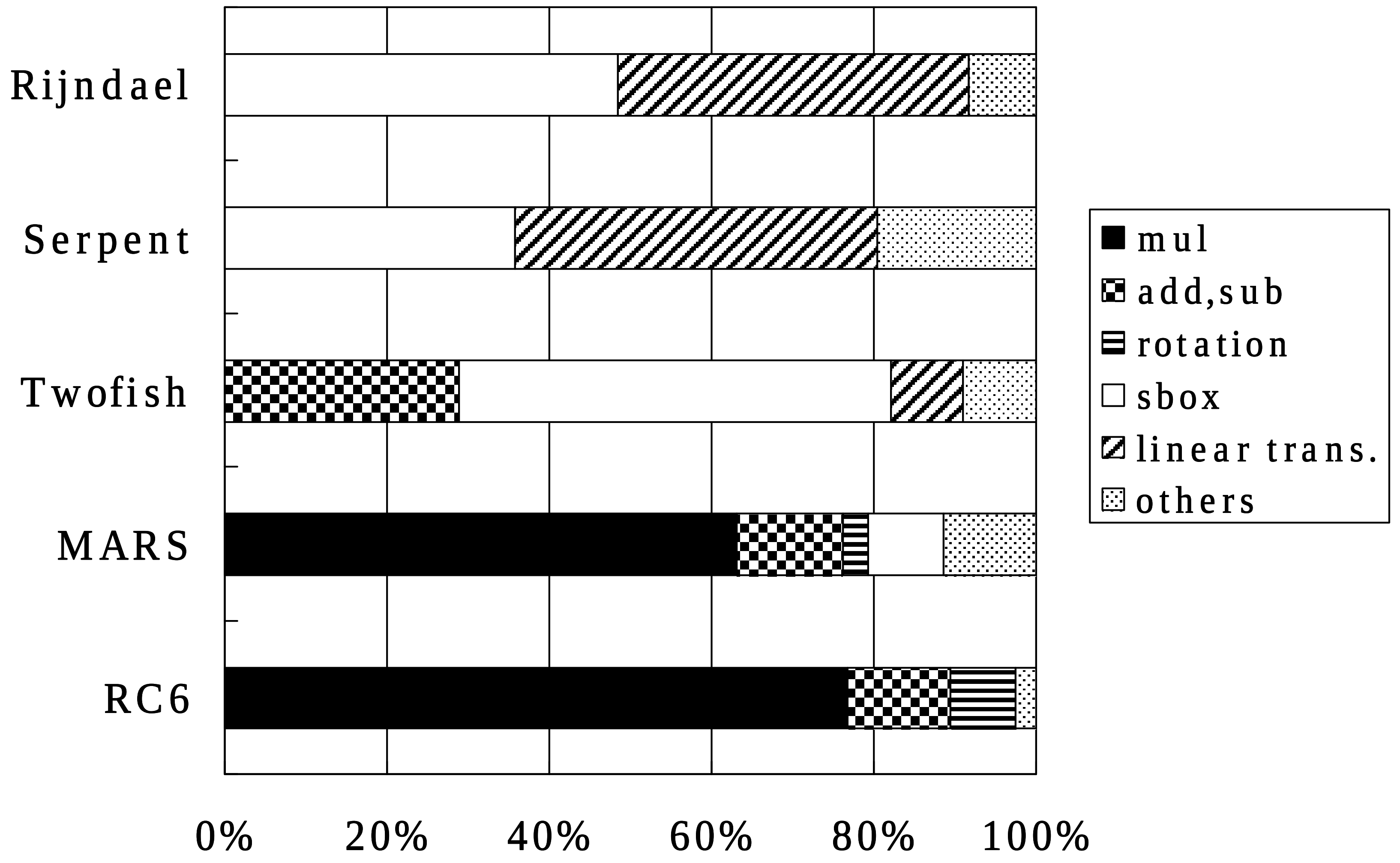
Hardware Evaluation Results

Algorithm name	Key setup time[ns]	critical-path[ns]	Throughput [Mbps]
DES	-	55.11	1161.31
Triple-DES	-	157.09	407.40
MARS	1741	567.49	225.55
RC6	2112.3	627.57	203.96
Rijndael	57.39	65.64	1950.03
Serpent	114.07	137.4	931.58
Twofish	16.38	324.8	394.08

- The details of hardware components on Critical path -

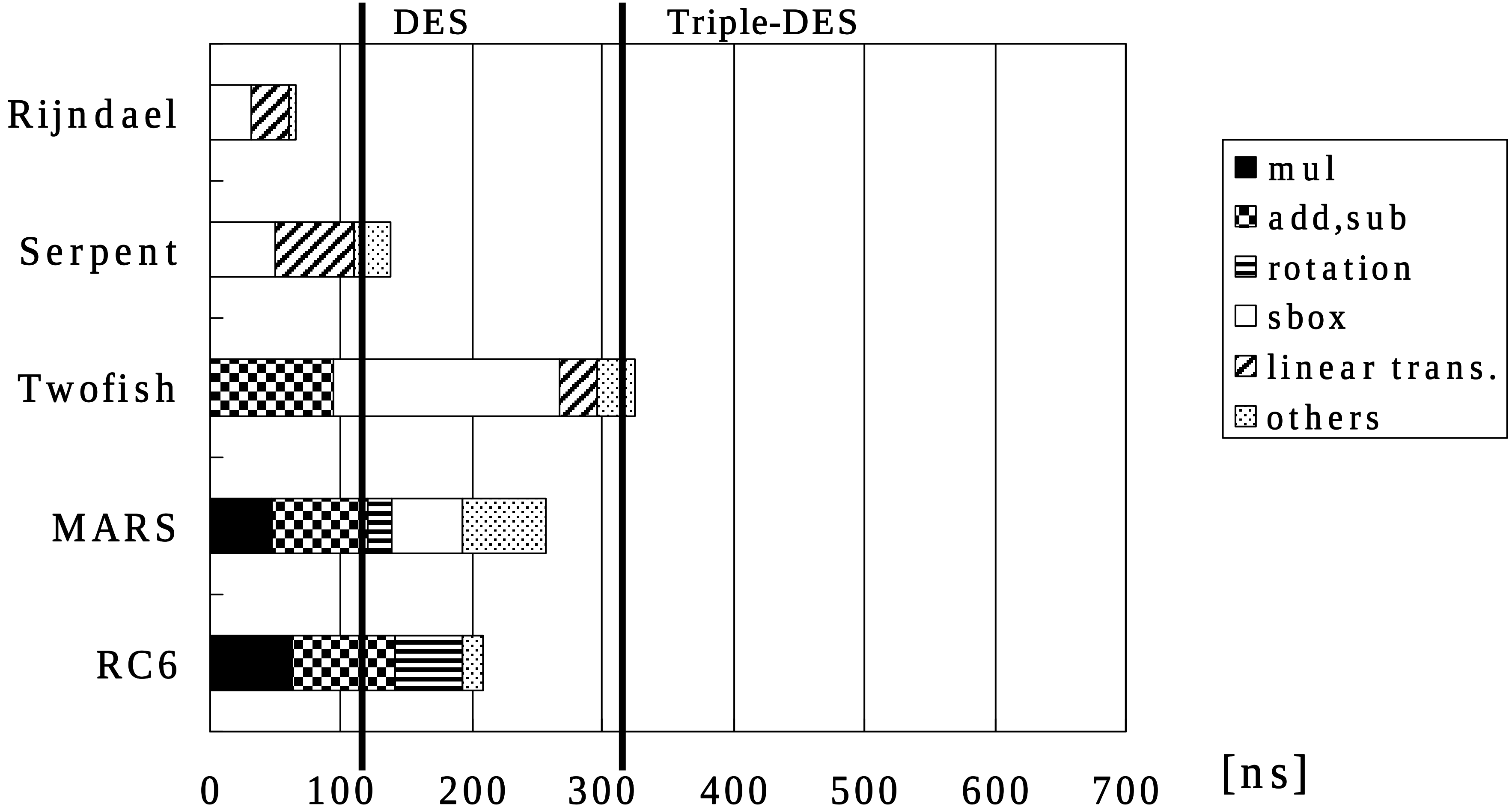


- The proportion of each component on Critical path -



Discussions

- an example of optimized multiplication -



Conclusions

* We evaluated the fastest possible encryption speed of the AES finalists (in feedback modes) using the existing hardware standard library under our design policies.

*Our evaluation results (encryption speed):

Rijndael > DES ≈ Serpent >
(≈ 2[Gbps]) (≈ 1[Gbps])

Triple-DES ≈ Twofish > Mars ≈ RC6
(≈ 400[Mbps]) (≈ 200[Mbps])